INSec#9 ネットワークの防御

- 要素技術
- ファイアウォール
  - 防火壁-防火戸付き
  - WIDE：ファイアウォール 基礎から応用 → http://www.soi.wide.ad.jp/class/20060031/slides/18/index_31.html
  - 実装方式
    - パケットフィルタ方式
      - TCP/IP通信
        - 対象
          - IPヘッダ情報：L3
            - 発信元および宛先のIPアドレス
            - 上位層プロトコルの種別(TCP、UDP、ICMP等)
            - オプション情報(パケット分割情報、ソースルーティング情報等)
          - 上位層ヘッダ情報：L4以上
            - 発信元及び宛先のポート番号：TCP/UDPの場合
            - ヘッダ上のフラグ類(TCPの場合、SYN、ACK、FIN等の状態制御フラグ)
            - ICMPタイプ(ICMPの場合)
        - 双方向通信
          - 発信元ポート番号は一定ではない。毎回変化する
            - 同じ宛先に複数の通信セッション
          - 応答パケットの宛先ポート番号 → 1024以上
            - 1024未満：グローバルなサービス
      - ダイナミックパケットフィルタ
        - アクセス制御リスト(ACL：Access Control List)
        - ACLに基づき個別の通信セッションごとに双方向通信許可
        - NAT内蔵FW-家庭用
          - UPnP(Universal Plug and Play)
        - ステートフル・インスペクション
          - 拡張機能
        - IP詐称の脅威
          - 絶対的な有効策なし
          - Ingress/Egressフィルタで一部対応
    - アプリケーションレベルゲートウェイ方式
      - 別名：プロキシ方式、サーキットレベルゲートウェイ方式、専用ゲートウェイ
      - パケットレベルでの中継機能を持たない
      - プロキシ(代理：Proxy)サーバ
        - 個別のプロトコルごと
          - HTTP Proxy
          - FTP Proxy
          - POP3 Proxy
        - さまざまな付加機能
        - 診断くん → http://taruo.net/e/
    - ハイブリッド方式
      - パケットフィルタをベース
        - UDP上のアプリケーション
        - 高いスループットが必要なプロトコル
      - 一部のプロトコルをプロキシ的に処理
        - ウイルス検査
    - 透過型プロキシサーバ
      - パケットフィルタ方式と同様の使い方
      - ゲートウェイ上で通信を横取り
        - 利用者からはその存在が見えない
      - アプリケーションレベルゲートウェイ方式製品、ハイブリッド方式製品に実装
    - サーキットレベルゲートウェイ方式
      - 別名：汎用ゲートウェイ、回線ゲートウェイ、トランスポート・ゲートウェイ
      - トランスポート層(サーキットレベル)での中継
      - 内容チェックなし、接続可否のチェックのみ
      - 単純にポート間でのデータ中継
        - ポートフォワーディング(Port Forwarding)
    - L2ファイアウォール
      - 別名：ブリッジモード、透過モード
      - データリンク層フレームの中継
        - FWの前後でIPアドレスが変わらない
      - L3以上の機能を除くFWの設定
  - ファイアウォールとUTM
    - UTM(Unified Threat Management)
      - 別名：統合型脅威管理
      - 複数の異なるセキュリティ機能を統合し、集中的にネットワーク管理を行うこと
    - 階層的防御モデル
      - マルウェア(脅威) →
        - ファイアウォール →
          - 侵入防御 →
            - アンチウイルス →
              - スパムフィルタ
              - URLフィルタ
    - FWの拡張としてのUTM
      - 統合
        - LANスイッチ
        - ルータ
        - ファイアウォール
        - …ネットワーク機器全て
      - 究極のネットワークレベルでのUTM
    - 相反する要求とコスト、実現可能性のバランス
      - 通信処理能力
      - 付加機能
        - ファイアウォール
        - 侵入防御
        - URL/コンテンツ検査
        - スパム対策
        - …
  - 導入設計
- 攻撃の検知と防御